Weekly Update

Week of July 10, 2017

Subject: Governance, Risk and Compliance: An Introduction for Procurement Directors and Professionals

Audience: Procurement Directors and Professionals (*For agencies that have not yet met with the SCEIS team regarding GRC implementation related to materials management).*

Governance, Risk and Compliance (GRC) is a current SCEIS project that is being implemented in partnership with all agencies. GRC will assist the State in adhering to the Segregation of Duties (SOD) policy established in 2014. This document was developed to provide South Carolina materials management professionals with the background of GRC, an overview of the current GRC project, and strategies for implementing GRC at their agencies.

Background of GRC

What is Segregation of Duties?

Segregation of Duties (SOD) serves as the basis for the current GRC project. SOD is an internal control that attempts to ensure that no single individual has the authority to execute two or more conflicting sensitive transactions with the potential to impact financial statements. The objective is to reduce the possibility of fraud in an agency and to have better controls in the organization of day-to-day operations. All sensitive end-to-end functions should be identified, and tasks associated with them should be distributed to one or more persons.

In order to meet SOD compliance, an agency should focus on the transactions that pose the greatest risk to the business and gain understanding of the issues related to access. Agency personnel should determine that appropriate steps are being taken to remedy and mitigate the root causes of the issues to an extent that satisfies management and audit parties.

Establishing adequate separation of duties requires an agency to:

1. **A**nalyze risk by reviewing roles assigned to users
2. **B**uild in controls to high risk transactions
3. **C**ommunicate changes in roles and user assignments (To this end, the SCEIS Team has implemented a process through which agencies designate a person or persons in the agency authorized to request role additions, deletions and changes. These individuals are called Data Owners and are responsible for communicating appropriately within the agency to ensure proper system access based on an employee's job duties).

This principle can be thought of as the "ABC's of Separation of Duties."

For more information on SOD, please refer to the SCEIS Segregation of Duties Policy.

Some useful appendices included in the SCEIS Segregation of Duties Policy are as follows:

- **Role Conflicts** - provides a concise list of roles by module that have conflicting roles
- **Detailed Role Conflict Descriptions/Tasks** - provides the more specific breakdown of each role, the conflicting roles, and the associated tasks

Note: Each agency is responsible for the appropriate review and assignment of system access.

Smaller agencies can find it impractical to have meaningful SOD based on limited staff. However, direct management involvement provides a strong deterrent to conflicting activities. Examples of such involvement include:

- Having a manager perform one aspect of the transaction (e.g. approving the shopping cart, etc.)
- Active review by management of financial data and reports
- A detailed management review of activities involving finances, inventory, and other assets as a compensating control activity

This kind of review and supervision can mitigate the risk of having one person responsible for several critical tasks in a smaller agency.

Overview of GRC

What is GRC?

The current GRC project is a result of a Deloitte Security and Privacy Assessment which recommended the implementation of a statewide GRC program that would enable the measurement of the security posture and progress at agency and statewide levels:

> The State and its agencies must comply with numerous requirements for the safeguarding of PII [Personally Identifiable Information], Protected Health Information (PHI), certain other sensitive data and reducing fraud … Implementing a GRC tool using an integrated strategy will improve the quality of data shared between professionals, drive consistency, help reduce risks, and accelerate the delivery of guidance and gathering of compliance data (Deloitte & Touche LLP, 2014).

The aim of GRC is to help an organization identify risks and effectively eliminate or mitigate them.

Essentially, there are three ways that GRC accomplishes this:

- Analyzing risks associated with user/roles
- Managing user assignments
- Monitoring user assignments

What is a Risk?

A simple example of a risk is a user having access to several process combinations such as the following:

- Assign roles/profiles to self
- Access to create a shopping cart and approve it, to create a Purchase Order and receive the goods
- Access to execute reports

If appropriate internal controls are not in place to mitigate risks, insufficiencies can lead to significant deficiencies and/or material weaknesses.

The analysis of the SCEIS environment to date indicates that most risks appear to be caused by the combination of role assignments to a particular user rather than by conflicting actions within an individual role. The following categories of duties or responsibilities, for example, are considered incompatible and must be separated:

- Initiating a transaction and approving the same transaction

Historically, agencies have managed risk in silos across different teams, processes, and methods. However, we understand today that people, processes, and technology should all work together to help an agency stay in control of the risks it chooses to take.

What is a Mitigation?

From a GRC perspective, a mitigation is something that an agency has in place or puts in place to minimize a risk when business conditions require personnel to have the opportunity to potentially exploit a weakness. Whenever a user/role has a risk and it is not possible to remove any authorization from the user, a mitigation control can be utilized. This is a process during which detective controls are put in place wherever preventive security controls are too restrictive to business operations. Therefore, you can use mitigation controls when it is not possible to segregate duties from the business process. Once mitigation is applied, it is valid for a 12-month period and then is subject to review to ensure that it is still valid and appropriate.

Weekly Update

Week of July 10, 2017

Implementation of GRC

How Do We Evaluate SOD Risk at My Agency?

Before adopting a mitigation control, agencies should conduct a review to ensure that the transactions and roles assigned are fully understood and correct.

It is incumbent upon each agency to ensure that appropriate review and assignment of system access be considered in light of the potential for fraudulent activity. Transactions are available to select procurement personnel and all agency Data Owners to assist in identifying roles assigned to specific positions include the following:

- Display user roles, zwf_user_roles
- Display user roles from ECC, SRM, BW, zsec_user_roles_comb

Also, it is advisable for your agencies data owner to request a current copy of your SRM Organizational Structure. This will better assist you with determining what roles can be removed from a user and when mitigation should be applied.

By reviewing the SRM Organizational Structure and role assignments within your agency you should gain insight into your agency's SOD risk and conflicts and be primed to identify the appropriate mitigating controls towards supporting the prioritization of the State's risk mitigation efforts.

What Are The Next Steps in Understanding GRC and Its Impact on My Agency?

It is important for your agency to understand and assess the landscape of current conflicts, reduce them to the extent possible via remediation initiatives, and apply mitigating controls to the remaining issues. This approach may not yield zero SOD conflicts, but your efforts will demonstrate that management has evaluated existing conflicts and reduced residual risks to an acceptable level through tested and controlled processes. Typically, this solution is palatable to auditors and regulators and promotes the awareness of risk beyond a compliance-only exercise.

To assist you in your agency's evaluation, the SCEIS GRC team has compiled agency-specific SOD documents that will identify the users at your agency who may have conflicts based on the multiple roles that they have been assigned. **SCEIS will contact you to provide these documents and set up meetings with your agency personnel to discuss specific questions that you may have and mitigation controls that may be put in place.**

Remember that the SCEIS team is in place to support the deployment, operation, and maintenance of SCEIS applications. The aim of the GRC project is to assist agencies in their efforts toward improving risk management activities, enabling your agency to

manage – but not entirely mitigate – risks, identified in a balanced and efficient way that reflects the value of your organization to the State of South Carolina.

We look forward to discussing the details of the GRC project in more depth with you and answering whatever questions you might have during individual agency meetings. **In the coming days, Laura McLendon, FI Project Coordinator, will contact agencies to schedule a MM GRC meeting.**

References:

Deloitte & Touche LLP (2014). *State of South Carolina Information Security and Privacy Final Report.* Retrieved from the South Carolina Department of Administration website: *http://www.admin.sc.gov/files/InfoSec%20-%20Public%20Final%20Report%20-%201Dec2014.pdf*